**EXHIBIT C-9**
**EXEMPLARY PORTIONS OF PRIOR ART THAT TEACH OR SUGGEST EACH ELEMENT OF THE ASSERTED '661 CLAIMS**
**PATENT L.R. 3-3(C)**

| **Claim 5 ('661 Patent)** | **U.S. 5,157,725 to Lindholm ("Lindholm '725")** |
|---|---|
| A cryptographic processing device for securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret by external monitoring, comprising: | 1:6-11 – "The present invention relates to a method and an apparatus for preventing external detection of signal information in video signals occurring in, and being emitted from, a display unit, or a similar unit, and comprising substantially consecutive frame or field signals each consisting of substantially consecutive line signals."<br><br>1:12-15 – "Display units are widely used as components in, for example, data processing systems in which confidential information is processed and stored, and also in similar units, such as matrix printers."<br><br>1:54-58 – "A first object of the present invention is to further improve the methods and the apparatuses of the type mentioned by way of the introduction to prevent, in actual practice, any type of external detection of the signal information in the video signals."<br><br>1:59-63 – "According to the present invention, external detection of the signal information in the video signals may be rendered even more difficult if the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits."<br><br>1:64-2:8 – "Although the video signal circuits are, conventionally, separated from the power supply line by means of a low-pass filter, the video signals can nevertheless by transmitted to the power supply line, e.g. a mains connection, and the signal information in the video signals may thus be detected on, for example, external lines connected to the power supply line. For lower frequencies, the power supply line may also serve as a part of the emitting construction if the power supply filtration of the display unit is insufficient, which is extremely common in commercial data terminal equipment. Thus, the video signals may be emitted from the power supply line."<br><br>2:36-43: "According to a second aspect of the invention, this is achieved in a method of the type described by way of the introduction in that the bit frequencies of the pseudo-random bit signal sequence/sequences are varied. In the apparatus according to the invention for carrying out said method, a control unit is used for varying the bit frequency of the pseudo-random bit signal |

| | |
|---|---|
| | sequence/sequences."<br><br>Claim 1 – "A method for preventing external detection of signal information in video signals comprising steps of:<br><br>a) emitting video signals containing a bit signal sequence from a video circuit;<br><br>b) generating a phantom signal with at least one pseudo-random bit signal sequence and having properties similar to the bit signal sequence of the video signals emitted from the video circuit;<br><br>c) varying bit frequencies of the pseudo-random bit signal sequence;<br><br>d) emitting the phantom signal in addition to the video signals via electromagnetic waves; and<br><br>e) supplying the phantom signal to an external power supply line connected to the video circuit." |
| (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |
| (b) a source of unpredictable information; | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal." |
| (c) a processor: | 3:46-56 – "The conventional display unit shown in FIG. 1 comprises a cathode ray tube 10 with deflection yokes 11, 12 and a sweep generator 13. On the input side, the display unit comprises a data register 14, a character type memory 15, and a parallel-to-serial |

| | |
|---|---|
| | converter 16. A pixel clock generator 17 is connected, via a divider 18, to the data register 14, as well as to the converter 16, and is, furthermore, directly connected to the latter. A display control unit 19 is also directly connected to the output of the generator 17, as well as to the sweep generator 13 for control thereof."<br><br>4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal." |
| (i) connected to said input interface for receiving and cryptographically processing said quantity, | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |
| (ii) configured to use said unpredictable information to conceal a correlation between externally monitorable signals and said secret during said processing of said quantity by randomizing the order of said permutation; and | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>2:36-43: "According to a second aspect of the invention, this is achieved in a method of the type described by way of the introduction in that the bit frequencies of the pseudo-random bit signal sequence/sequences are varied. In the apparatus according to the invention for carrying out said method, a control unit is used for varying the bit frequency of the pseudo-random bit signal sequence/sequences." |

| | |
|---|---|
| | Claim 1 – "A method for preventing external detection of signal information in video signals comprising steps of:<br><br>a) emitting video signals containing a bit signal sequence from a video circuit;<br><br>b) generating a phantom signal with at least one pseudo-random bit signal sequence and having properties similar to the bit signal sequence of the video signals emitted from the video circuit;<br><br>c) varying bit frequencies of the pseudo-random bit signal sequence;<br><br>d) emitting the phantom signal in addition to the video signals via electromagnetic waves; and<br><br>e) supplying the phantom signal to an external power supply line connected to the video circuit." |
| (d) an output interface for outputting said cryptographically processed quantity to a recipient thereof. | 3:68-4:2 – "This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam."<br><br>4:40-41 – "A line 20' serving as aerial may be connected to the output of the converter 16'." |

| **Claim 6 ('661 Patent)** | **U.S. Patent No. 5,157,725 to Lindholm ("Lindholm '725")** |
|---|---|
| A cryptographic processing device implemented on a single microchip for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external monitoring, comprising: | 1:6-11 – "The present invention relates to a method and an apparatus for preventing external detection of signal information in video signals occurring in, and being emitted from, a display unit, or a similar unit, and comprising substantially consecutive frame or field signals each consisting of substantially consecutive line signals."<br><br>1:12-15 – "Display units are widely used as components in, for example, data processing systems in which confidential information is processed and stored, and also in similar units, such as matrix printers."<br><br>1:54-58 – "A first object of the present invention is to further improve the methods and the apparatuses of the type mentioned by way of the introduction to prevent, in actual practice, any type of external detection of the signal information in the video signals."<br><br>1:59-63 – "According to the present invention, external detection of the signal information in the video signals may be rendered even more difficult if the phantom signal is also supplied on an external power |

| | |
|---|---|
| | supply line to the unit containing the video signal circuits."<br><br>1:64-2:8 – "Although the video signal circuits are, conventionally, separated from the power supply line by means of a low-pass filter, the video signals can nevertheless by transmitted to the power supply line, e.g. a mains connection, and the signal information in the video signals may thus be detected on, for example, external lines connected to the power supply line. For lower frequencies, the power supply line may also serve as a part of the emitting construction if the power supply filtration of the display unit is insufficient, which is extremely common in commercial data terminal equipment. Thus, the video signals may be emitted from the power supply line."<br><br>Claim 1 – "A method for preventing external detection of signal information in video signals"<br><br>Scott Guthery, "Smart Cards," May 28, 1998, www.usenix.org/publications/login/1998-5/guthery.html (visited Dec. 5, 2006) ("Single-chip smart card processors based on these cores are made by almost all the large silicon foundries . . . .Several marketplace forces are at work to open the smart card as a general-purpose computing platform.").<br><br>*See generally* U.S. Patent No. 5,944,833 to Ugon. |
| (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |
| (b) a source of unpredictable information; | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and |

| | |
|---|---|
| | 16 and forming a generator for generating the phantom signal." |
| (c) a processor: | 3:46-56 – "The conventional display unit shown in FIG. 1 comprises a cathode ray tube 10 with deflection yokes 11, 12 and a sweep generator 13. On the input side, the display unit comprises a data register 14, a character type memory 15, and a parallel-to-serial converter 16. A pixel clock generator 17 is connected, via a divider 18, to the data register 14, as well as to the converter 16, and is, furthermore, directly connected to the latter. A display control unit 19 is also directly connected to the output of the generator 17, as well as to the sweep generator 13 for control thereof."<br><br>4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal." |
| (i) connected to said input interface for receiving and cryptographically processing said quantity, | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |
| (ii) configured to use said unpredictable information to conceal a correlation between said microchip's power consumption and said processing of said quantity by expending additional electricity | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>5:14-27 – "As is plain from FIG. 3, power is fed to the video signal circuits via the apparatus according to the invention. Thus, the |

| | |
|---|---|
| in said microchip during said processing; and | phantom signal generator C is adapted to feed the phantom signal not only to the aerial E, but also to the power feed connection F via the mains filter D. Despite the attenuation of the phantom signal in the mains filter D, the phantom signal can be given a much higher effect than the leaking video signals, via the apparatus B according to the invention, from the video signal circuits to the power supply line F. Thus, the total output to the power supply line F can be rendered smaller or, at the most, about as large as the previous output to this line without the use of the invention."<br><br>5:31-60 – "The embodiment shown in FIG. 4 of the apparatus according to the invention is advantageously combined with the embodiment of FIG. 3 and generates three pseudo-random bit signal sequences with properties similar to those of the video signals. Three random number generators 21-23, each for example consisting of a maximum recurrence length shift register, generate these three pseudo-random bit signal sequences with the bit frequencies f1, f2 and f3, respectively, which are determined by oscillators 24-26 connected to their respective random number generator 21-23 via frequency modulators 27-29. These modulators modulate the output signal from the oscillators 24-26 with a frequency, preferably the line frequency of the display unit, in that they are connected to a synchronisation circuit 30 whose output signal has said line frequency. This is achieved, more precisely, by the use of a sensing loop 31 sensing the signals in the deflection yokes of the cathode ray tube and applying a corresponding voltage to the synchronisation circuit. From this voltage, the synchronisation circuit 30 derives the line frequency and thus feeds a signal of this frequency to the modulation inputs of the modulators 27-29 but also to a divider 32 whose output is connected to the reset outputs of the random number generators 21-23. Via amplifiers 33-35, adaptation units 36-38, cables 39-41, and further adaptation units 42-44, the outputs of the random number generators 21-23 are connected to one aerial 45-47 each." |
| (d) an output interface for outputting said cryptographically processed quantity to a recipient thereof. | 3:68-4:2 – "This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam."<br><br>4:40-41 – "A line 20' serving as aerial may be connected to the output of the converter 16'." |

| **Claim 11 ('661 Patent)** | **U.S. Patent No. 5,157,725 to Lindholm** |
|---|---|
| A cryptographic | 1:6-11 – "The present invention relates to a method and an apparatus |

| | |
|---|---|
| processing device for securely performing a cryptographic processing operation in a manner resistant to discovery of a secret by external measurement of said device's power consumption, comprising: | for preventing external detection of signal information in video signals occurring in, and being emitted from, a display unit, or a similar unit, and comprising substantially consecutive frame or field signals each consisting of substantially consecutive line signals."<br><br>1:12-15 – "Display units are widely used as components in, for example, data processing systems in which confidential information is processed and stored, and also in similar units, such as matrix printers."<br><br>1:54-58 – "A first object of the present invention is to further improve the methods and the apparatuses of the type mentioned by way of the introduction to prevent, in actual practice, any type of external detection of the signal information in the video signals."<br><br>1:59-63 – "According to the present invention, external detection of the signal information in the video signals may be rendered even more difficult if the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits."<br><br>1:64-2:8 – "Although the video signal circuits are, conventionally, separated from the power supply line by means of a low-pass filter, the video signals can nevertheless by transmitted to the power supply line, e.g. a mains connection, and the signal information in the video signals may thus be detected on, for example, external lines connected to the power supply line. For lower frequencies, the power supply line may also serve as a part of the emitting construction if the power supply filtration of the display unit is insufficient, which is extremely common in commercial data terminal equipment. Thus, the video signals may be emitted from the power supply line."<br><br>Claim 1 – "A method for preventing external detection of signal information in video signals" |
| (a) an input interface for receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |

| | |
|---|---|
| (b) an input interface for receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; | 5:14-27 – "As is plain from FIG. 3, power is fed to the video signal circuits via the apparatus according to the invention. Thus, the phantom signal generator C is adapted to feed the phantom signal not only to the aerial E, but also to the power feed connection F via the mains filter D. Despite the attenuation of the phantom signal in the mains filter D, the phantom signal can be given a much higher effect than the leaking video signals, via the apparatus B according to the invention, from the video signal circuits to the power supply line F. Thus, the total output to the power supply line F can be rendered smaller or, at the most, about as large as the previous output to this line without the use of the invention." |
| (c) a processor connected to said input interface for receiving and cryptographically processing said quantity; and | 3:46-56 – "The conventional display unit shown in FIG. 1 comprises a cathode ray tube 10 with deflection yokes 11, 12 and a sweep generator 13. On the input side, the display unit comprises a data register 14, a character type memory 15, and a parallel-to-serial converter 16. A pixel clock generator 17 is connected, via a divider 18, to the data register 14, as well as to the converter 16, and is, furthermore, directly connected to the latter. A display control unit 19 is also directly connected to the output of the generator 17, as well as to the sweep generator 13 for control thereof."<br><br>3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam."<br><br>4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal." |
| (d) a noise production system for | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more |

| | |
|---|---|
| introducing noise into said measurement of said power consumption. | difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>4:60-68 – "Although the above generator is utilised for generating the phantom signal, it has been proven possible to externally detect the information in the video signals occurring in a display unit. According to a first aspect of the invention, such detection can be rendered even more difficult when the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits, as shown in, for instance, FIG. 3." |

| **Claim 12 ('661 Patent)** | **U.S. 5,157,725 to Lindholm** |
|---|---|
| The device of claim 11 wherein said noise production system comprises: (a) a source of randomness for generating initial noise having a random characteristic; | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>4:60-68 – "Although the above generator is utilised for generating the phantom signal, it has been proven possible to externally detect the information in the video signals occurring in a display unit. According to a first aspect of the invention, such detection can be rendered even more difficult when the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits, as shown in, for instance, FIG. 3." |
| (b) a noise processing module for improving the random characteristic of said initial noise; and | 5:19-27 – "Despite the attenuation of the phantom signal in the mains filter D, the phantom signal can be given a much higher effect than the leaking video signals, via the apparatus B according to the invention, from the video signal circuits to the power supply line F. Thus, the total output to the power supply line F can be rendered smaller or, at the most, about as large as the previous output to this line without the use of the invention." |

| | |
|---|---|
| | 6:15-18 – "According to the invention, the phantom signal can be altered from one frame or field period to the next, at the same time as the corresponding video signal is changed." |
| (c) a noise production module configured to vary said power consumption based on an output of said noise processing module. | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>4:60-68 – "Although the above generator is utilised for generating the phantom signal, it has been proven possible to externally detect the information in the video signals occurring in a display unit. According to a first aspect of the invention, such detection can be rendered even more difficult when the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits, as shown in, for instance, FIG. 3." |

| **Claim 28 ('661 Patent)** | **U.S. 5,157,725 to Lindholm** |
|---|---|
| A method of securely performing a cryptographic processing operation implementing a permutation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring, comprising: | 1:6-11 – "The present invention relates to a method and an apparatus for preventing external detection of signal information in video signals occurring in, and being emitted from, a display unit, or a similar unit, and comprising substantially consecutive frame or field signals each consisting of substantially consecutive line signals."<br><br>1:12-15 – "Display units are widely used as components in, for example, data processing systems in which confidential information is processed and stored, and also in similar units, such as matrix printers."<br><br>1:54-58 – "A first object of the present invention is to further improve the methods and the apparatuses of the type mentioned by way of the introduction to prevent, in actual practice, any type of external detection of the signal information in the video signals."<br><br>1:59-63 – "According to the present invention, external detection of the signal information in the video signals may be rendered even more difficult if the phantom signal is also supplied on an external power |

| | |
|---|---|
| | supply line to the unit containing the video signal circuits."<br><br>1:64-2:8 – "Although the video signal circuits are, conventionally, separated from the power supply line by means of a low-pass filter, the video signals can nevertheless by transmitted to the power supply line, e.g. a mains connection, and the signal information in the video signals may thus be detected on, for example, external lines connected to the power supply line. For lower frequencies, the power supply line may also serve as a part of the emitting construction if the power supply filtration of the display unit is insufficient, which is extremely common in commercial data terminal equipment. Thus, the video signals may be emitted from the power supply line."<br><br>2:36-43: "According to a second aspect of the invention, this is achieved in a method of the type described by way of the introduction in that the bit frequencies of the pseudo-random bit signal sequence/sequences are varied. In the apparatus according to the invention for carrying out said method, a control unit is used for varying the bit frequency of the pseudo-random bit signal sequence/sequences."<br><br>Claim 1 – "A method for preventing external detection of signal information in video signals comprising steps of:<br><br>a) emitting video signals containing a bit signal sequence from a video circuit;<br><br>b) generating a phantom signal with at least one pseudo-random bit signal sequence and having properties similar to the bit signal sequence of the video signals emitted from the video circuit;<br><br>c) varying bit frequencies of the pseudo-random bit signal sequence;<br><br>d) emitting the phantom signal in addition to the video signals via electromagnetic waves; and<br><br>e) supplying the phantom signal to an external power supply line connected to the video circuit." |
| (a) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output |

| | |
|---|---|
| | signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |
| (b) generating unpredictable information; | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal." |
| (c) using said unpredictable information while processing said quantity to conceal a correlation between externally monitorable signals and said secret by randomizing the order of said permutation; and | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>2:36-43: "According to a second aspect of the invention, this is achieved in a method of the type described by way of the introduction in that the bit frequencies of the pseudo-random bit signal sequence/sequences are varied. In the apparatus according to the invention for carrying out said method, a control unit is used for varying the bit frequency of the pseudo-random bit signal sequence/sequences."<br><br>Claim 1 – "A method for preventing external detection of signal information in video signals comprising steps of:<br><br>a) emitting video signals containing a bit signal sequence from a video circuit;<br><br>b) generating a phantom signal with at least one pseudo-random bit signal sequence and having properties similar to the bit signal sequence of the video signals emitted from the video circuit;<br><br>c) varying bit frequencies of the pseudo-random bit signal sequence;<br><br>d) emitting the phantom signal in addition to the video signals via electromagnetic waves; and |

| | |
|---|---|
| | e) supplying the phantom signal to an external power supply line connected to the video circuit." |
| (d) outputting said cryptographically processed quantity to a recipient thereof. | 3:68-4:2 – "This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam."<br><br>4:40-41 – "A line 20' serving as aerial may be connected to the output of the converter 16'." |

| **Claim 29 ('661 Patent)** | **U.S. Patent No. 5,157,725 to Lindholm** |
|---|---|
| A method of securely performing a cryptographic processing operation in a manner resistant to discovery of a secret within a cryptographic processing device by external monitoring of said device's power consumption, comprising: | 1:6-11 – "The present invention relates to a method and an apparatus for preventing external detection of signal information in video signals occurring in, and being emitted from, a display unit, or a similar unit, and comprising substantially consecutive frame or field signals each consisting of substantially consecutive line signals."<br><br>1:12-15 – "Display units are widely used as components in, for example, data processing systems in which confidential information is processed and stored, and also in similar units, such as matrix printers."<br><br>1:54-58 – "A first object of the present invention is to further improve the methods and the apparatuses of the type mentioned by way of the introduction to prevent, in actual practice, any type of external detection of the signal information in the video signals."<br><br>1:59-63 – "According to the present invention, external detection of the signal information in the video signals may be rendered even more difficult if the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits."<br><br>1:64-2:8 – "Although the video signal circuits are, conventionally, separated from the power supply line by means of a low-pass filter, the video signals can nevertheless by transmitted to the power supply line, e.g. a mains connection, and the signal information in the video signals may thus be detected on, for example, external lines connected to the power supply line. For lower frequencies, the power supply line may also serve as a part of the emitting construction if the power supply filtration of the display unit is insufficient, which is extremely common in commercial data terminal equipment. Thus, the video signals may be emitted from the power supply line."<br><br>Claim 1 – "A method for preventing external detection of signal |

| | |
|---|---|
| | information in video signals" |
| (a) receiving a variable amount of power, said power consumption varying measurably during said performance of said operation; | 5:14-27 – "As is plain from FIG. 3, power is fed to the video signal circuits via the apparatus according to the invention. Thus, the phantom signal generator C is adapted to feed the phantom signal not only to the aerial E, but also to the power feed connection F via the mains filter D. Despite the attenuation of the phantom signal in the mains filter D, the phantom signal can be given a much higher effect than the leaking video signals, via the apparatus B according to the invention, from the video signal circuits to the power supply line F. Thus, the total output to the power supply line F can be rendered smaller or, at the most, about as large as the previous output to this line without the use of the invention." |
| (b) receiving a quantity to be cryptographically processed, said quantity being representative of at least a portion of a message; | 3:57-4:2 – "On a character data bus, the data register 14 receives data concerning the characters to be shown on the display unit and transfers these data to the character type memory 15 which, for every character line to be shown on the display unit, generates a consecutive sequence of parallel bit signals which, one by one, are fed to the parallel-to-serial converter 16. For every line made by the sweep generator 13 on the display unit 10, the parallel-to-serial converter 16 emits a bit signal sequence with a bit configuration corresponding to the parts in question of the characters of the character line. This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam." |
| (c) introducing noise into said measurement of said power consumption while processing said quantity; and | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal. A line 20' serving as aerial may be connected to the output of the converter 16'."<br><br>4:60-68 – "Although the above generator is utilised for generating the phantom signal, it has been proven possible to externally detect the information in the video signals occurring in a display unit. According to a first aspect of the invention, such detection can be rendered even more difficult when the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits, as shown in, for instance, FIG. 3." |

| | |
|---|---|
| (d) outputting said cryptographically processed quantity to a recipient thereof. | 3:68-4:2 – "This output signal from the parallel-to-serial converter 16 is fed, via an amplifier, to the cathode ray tube 10 for intensity modulation of its electron beam."<br><br>4:40-41 – "A line 20' serving as aerial may be connected to the output of the converter 16'." |

| **Claim 30 ('661 Patent)** | **U.S. 5,157,725 to Lindholm** |
|---|---|
| The method of claim 29 wherein said step of introducing noise comprises: (a) generating initial noise having a random characteristic; | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>4:60-68 – "Although the above generator is utilised for generating the phantom signal, it has been proven possible to externally detect the information in the video signals occurring in a display unit. According to a first aspect of the invention, such detection can be rendered even more difficult when the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits, as shown in, for instance, FIG. 3." |
| (b) improving the random characteristic of said initial noise; and | 5:19-27 – "Despite the attenuation of the phantom signal in the mains filter D, the phantom signal can be given a much higher effect than the leaking video signals, via the apparatus B according to the invention, from the video signal circuits to the power supply line F. Thus, the total output to the power supply line F can be rendered smaller or, at the most, about as large as the previous output to this line without the use of the invention."<br><br>6:15-18 – "According to the invention, the phantom signal can be altered from one frame or field period to the next, at the same time as the corresponding video signal is changed." |
| (c) varying said power consumption based on said improved initial noise. | 4:29-39 – "To make external detection of the video signals emitted from the line 20 and from other parts of the video signal circuits more difficult, a phantom signal in the form of at least one pseudo-random bit signal sequence with properties similar to those of the video signals may be emitted from the display unit. For this purpose, a |

| | |
|---|---|
| | second character type memory 15' and a second parallel-to-serial converter 16' can be arranged in per se known manner, said memory and converter being controlled by the same signals as the units 15 and 16 and forming a generator for generating the phantom signal."<br><br>4:60-68 – "Although the above generator is utilised for generating the phantom signal, it has been proven possible to externally detect the information in the video signals occurring in a display unit. According to a first aspect of the invention, such detection can be rendered even more difficult when the phantom signal is also supplied on an external power supply line to the unit containing the video signal circuits, as shown in, for instance, FIG. 3." |